Monthly Cybersecurity Tips Newsletter
VOLUME 17, ISSUE 7• July 2022

Take Small Steps to Secure Your Identity Online

From the desk of Karen Sorady

VP for MS-ISAC Member Engagement

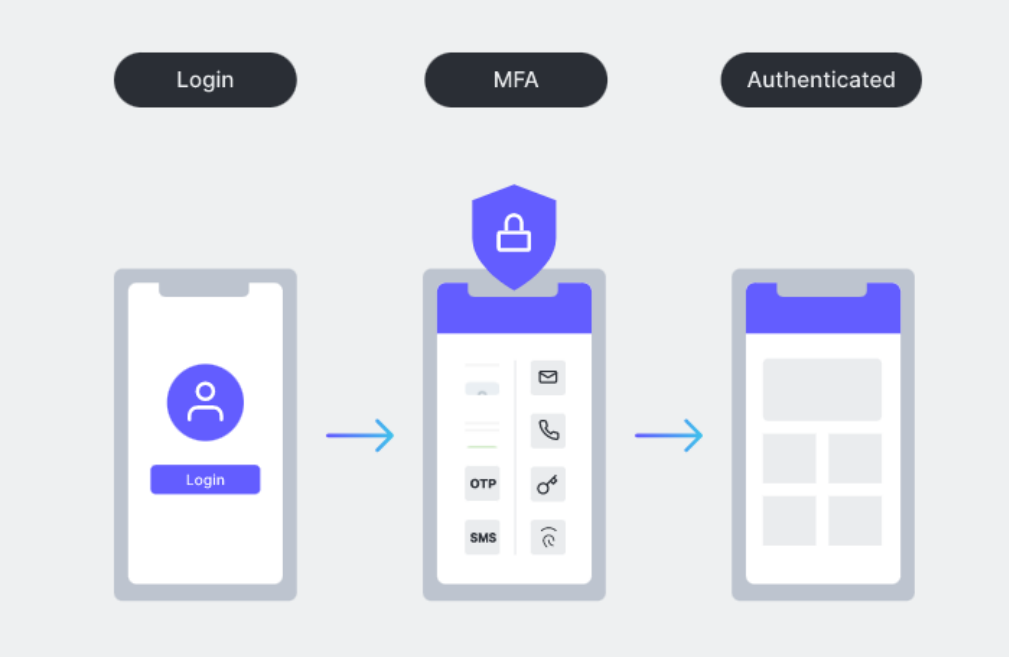
Have you ever taken a tally of every account you're signed up with? According to a 2021 study done by NordPass, the average person has about 100 passwords and associated accounts (i.e., credentials). Whether or not these accounts are active, we all run the risk of having this information exposed and misused. Given this shocking average, we can take easy steps to ensure our information is protected in cyberspace. While use of multi-factor authentication (MFA) can mitigate the threat of credential misuse by requiring at least two pieces of evidence (e.g., password and code sent to mobile phone) to confirm a user's identity, not all organizations or users have adopted this preferred method of authentication. When MFA is not yet available, the simplest action we can take is to make informed choices when creating passwords, including what mode of protection we apply to them. Because there's no rest for the wicked, cybercriminals are constantly finding new ways to circumvent what were previously thought to be secure online environments.

Why you should be using a password manager: A secure way to store your passwords is to use an electronic password manager that allows the use of multi-factor-authentication. Not only can a password manager generate strong passwords, but it can also hide them from view. Many password managers will only allow you to view your passwords via multi-factor authentication. The password manager also generates completely unique and long passwords without you having to come up with one on your own, and it stores each unique password for future use. Computers are much better at randomizing characters than humans, so you can rest easy knowing you aren't inadvertently re-using character patterns – which is a big password no-no. Those previously mentioned 100 passwords likely won't be learned by heart, and that's okay, as your password manager has your back! Below are forms of multi-factor-authentication that can be utilized with a password manager to add that extra layer of protection:

- **Voice call:** Exactly what it sounds like – you can opt in to receive verification calls from many password managers to confirm your identity.

- **Biometrics:** This is a technology that uses fingerprint or facial recognition software.
- **Push:** You can download corresponding apps on your phone or laptop that will trigger a notification to click on and verify identity.
- **Hardware token:** This is a small device that is either connected to or separate from your password manager. It generates a randomized code.
- **Email:** You receive an email as a form of identity confirmation.
- **SMS:** Similar to a push notification, you receive a text message to verify identity.

We all have a lot to worry about these days, but taking a small amount of time to research and activate a password manager can help us avoid at least one type of online vulnerability. You don't have to do much to become cyber-savvy either, as having and using the right tools is sometimes all you need.



Special thanks to Emma Kipniss, Education and Awareness Working Group Chair, for providing the content for this newsletter.